

Coherent state exchange in multi-prover quantum interactive proof systems

Debbie Leung*

Ben Toner[†]John Watrous[‡]

April 25, 2008

Abstract

We show that any number of parties can coherently exchange any one pure quantum state for another, without communication, given prior shared entanglement. Two applications of this fact to the study of multi-prover quantum interactive proof systems are given. First, we prove that there exists a one-round two-prover quantum interactive proof system for which no finite amount of shared entanglement allows the provers to implement an optimal strategy. More specifically, for every fixed input string, there exists a sequence of strategies for the provers, with each strategy requiring more entanglement than the last, for which the probability for the provers to convince the verifier to accept approaches 1. It is not possible, however, for the provers to convince the verifier to accept with certainty with a finite amount of shared entanglement. The second application is a simple proof that multi-prover quantum interactive proofs can be transformed to have near-perfect completeness by the addition of one round of communication.

1 Introduction

The idea that entanglement may be used as a resource is central to the theory of quantum communication and cryptography. Well-known examples include teleportation [BBC⁺93] and the superdense coding of both classical and quantum data [BW92, BSST02, HHL04]. In cryptography, entanglement is used not only in some implementations of quantum key-distribution [Eke91], but also as a mathematical tool in security proofs [LC99, SP00] of quantum key-distribution protocols not based on entanglement (such as [BB84]). In these settings it may be said that the relationship between entanglement and other resources (in particular quantum communication, classical communication, and private shared randomness) is reasonably well-understood [BDSW96, DHW04].

There are, on the other hand, settings of interest where the properties of entanglement as a resource are very poorly understood. One example can be found in quantum communication complexity, wherein it is not known if prior shared entanglement ever gives an asymptotic reduction in the number of qubits of communication required to solve general communication problems [Wol02, Bra03]. A second example, which is the main focus of this paper, concerns the power of entanglement in the multi-prover interactive proof system model, which has been studied in several recent papers [KM03, CHTW04, Weh06, CSUU07, CGJ07, KKM⁺07, KRT07]. Bell inequalities

*Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada.

[†]Centrum voor Wiskunde en Informatica, Amsterdam, The Netherlands.

[‡]Institute for Quantum Computing and School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada.

[Bel64, CHSH69], and many of the open problems concerning them [Gis07], have a fundamental connection to this model (although not necessarily to our main results).

Multi-prover interactive proof systems, which were first defined by Ben-Or, Goldwasser, Kilian, and Wigderson [BOGKW88], involve interactions among a *verifier* and two or more *provers*. The verifier is always assumed to be efficiently implementable, while the provers are typically permitted to have arbitrary complexity. The verifier and provers each receive a copy of some input string x , and then engage in an interaction based on this string. During this interaction the verifier communicates privately with each of the provers, possibly over the course of many rounds of communication, but the provers are forbidden from communicating directly with one another. The provers may, however, agree on a joint strategy before the interaction begins.

The provers act in collaboration to convince the verifier that the input string x is a *yes-input* to some fixed problem, and therefore should be *accepted*. The provers are not, however, considered to be trustworthy, and so the verifier must be defined in such a way that it *rejects* strings that are *no-inputs* to the problem being considered. These two conditions—that the provers can convince the verifier to accept yes-inputs but cannot convince the verifier to accept no-inputs—are called the *completeness* and *soundness* conditions, respectively, and are analogous to the notions in mathematical logic that share these names. In contrast to the notion of a mathematical proof, however, one typically requires only that the completeness and soundness conditions for interactive proof systems hold with high probability (for every fixed yes or no input string).

The study of interactive proof systems, including single-prover and multi-prover models, has had an enormous impact on the fields of computational complexity and theoretical cryptography [AB06, Gol01]. In particular, multi-prover interactive proof systems, and the characterization of their expressive power [BFL91], led to the discovery of the *PCP* (or *Probabilistically Checkable Proof*) *Theorem* [ALM⁺98, AS98, Din07], which was a critical breakthrough in understanding the hardness of approximation problems.

In the quantum setting, one must consider the possibility that the provers initially share entanglement, which they might use as part of their strategy during the interaction. With this seemingly small change, nearly everything we know about classical multi-prover interactive proof systems becomes invalid within the quantum model. The following points illustrate the effect of this change on our current state of knowledge.

- When the provers are not allowed to share prior entanglement, it is known that the class of promise problems that have multi-prover interactive proof systems is precisely NEXP, the class of problems that can be solved nondeterministically in exponential time. This holds for both classical [BFL91] and quantum [KM03] multi-prover interactive proofs.
- There are no nontrivial bounds known for the class of promise problems having multi-prover interactive proofs when the provers initially share entanglement, including the cases of both a classical and quantum verifier. At one extreme, such proof systems could have the same expressive power as single-prover interactive proof systems, and at the other extreme it is possible that uncomputable problems have such proof systems.

One very basic question about multi-prover interactive proofs with entangled provers has remained unanswered, and is closely related to the lack of good upper bounds on their power: *For a given verifier and input string, how much entanglement is needed for the provers to play optimally?* To obtain an upper bound on the expressive power of multi-prover interactive proofs with entangled provers, one seeks a general bound: a limit on the amount of entanglement, as a function of the verifier’s description and the given input, needed for the provers to play optimally.

Our first main result explains the difficulty in answering this question: we prove that there exist two-prover quantum interactive proof systems for which no finite amount of entanglement allows for an optimal strategy on any fixed input. In other words, there are interactive proofs such that, no matter what entangled state the provers choose on a given input, it would always be possible for them to do strictly better with more entanglement. There is, therefore, no strict upper bound of the form discussed above. This fact has an obvious but important implication: one must consider upper bounds on entanglement for *close-to-optimal* strategies if this approach is to yield upper bounds on the power of multi-prover quantum interactive proofs.

Our second main result concerns methods to achieve *perfect completeness* of quantum interactive proof systems while retaining small soundness error. In the single-prover case, an efficient transformation for doing this exists that is both simple and easy to analyze [KW00]. In the multi-prover setting, an analogous result was recently obtained by Kempe, Kobayashi, Matsumoto, and Vidick [KKMV08] based on a much more complicated transformation and analysis. This more complicated transformation was designed to handle the locality constraints imposed on multiple provers. It turns out, however, that this complicated procedure is not needed after all, provided one is willing to make a small sacrifice. We prove that the simple single-prover technique can be applied in the multi-prover case to yield a proof system with *near-perfect* completeness: honest provers are able to convince the verifier to accept yes-inputs with any probability smaller than 1 that they desire—but they might never reach probability 1 using finite resources. (For instance, the provers may choose to cause the verifier to accept yes-inputs with probability $1 - \varepsilon(n)$ where $\varepsilon(n)$ is the reciprocal of the busy beaver function. The implementation of such a strategy, however, could require an enormous amount of prior shared entanglement.)

The two main results just discussed are connected by the notion of *coherent state exchange*, which is discussed in the next section. The first main result is then proved in Section 3, while the second is proved in Section 4. The paper concludes with Section 5. Throughout the paper we assume the reader is familiar with quantum computing and with basic aspects of classical and quantum interactive proof systems. Our notation and terminology are consistent with other papers on these topics.

2 Coherent state exchange

We begin by defining *coherent state exchange* as follows. Consider m players P_1, \dots, P_m ; and suppose, for each $i \in \{1, \dots, m\}$, that player P_i holds a quantum system whose associated Hilbert space is denoted \mathcal{X}^i . The spaces \mathcal{X}^i and \mathcal{X}^j need not have equal dimension for $i \neq j$. For two chosen pure states $|\phi\rangle, |\psi\rangle \in \mathcal{X}^1 \otimes \dots \otimes \mathcal{X}^m$, we consider the situation in which the players wish to transform a shared copy of $|\phi\rangle$ into $|\psi\rangle$, or vice-versa. We require that this task is completed (1) *without communication* and (2) *by a coherent process*.

To say that a process that performs state exchange is *coherent* means that it can be applied in a way that preserves superpositions. In particular, this means that it is possible for the players to implement a transformation of the form

$$\alpha |0^m\rangle |\gamma\rangle + \beta |1^m\rangle |\phi\rangle \mapsto \alpha |0^m\rangle |\gamma\rangle + \beta |1^m\rangle |\psi\rangle,$$

where the first m qubits represent control qubits, with one held by each player, and where the state $|\gamma\rangle \in \mathcal{X}^1 \otimes \dots \otimes \mathcal{X}^m$ represents an arbitrary state shared by the players.

In the absence of additional resources, it is not possible in general to perform this task when $m \geq 2$. In particular, given that the players cannot create entanglement out of thin air, the task is easily seen to be impossible when the target state $|\psi\rangle$ has more entanglement than the initial

state $|\phi\rangle$. However, if we consider the situation in which the players initially share an auxiliary quantum state, and we allow this state to be perturbed slightly by the process, then the above impossibility argument based on entanglement is no longer valid—and as we will show, the task indeed becomes possible. We note that the coherence condition requires that a process of this sort to leave the auxiliary quantum state nearly unchanged, in essence using it as a catalyst. The players cannot, for instance, simply swap the input state $|\phi\rangle$ with an initially shared copy of $|\psi\rangle$ without losing coherence.

For the case of $m = 2$, one solution to this problem can be obtained through the use of van Dam and Hayden's *quantum state embezzlement* [DH03]. In quantum state embezzlement, two parties (Alice and Bob) perform a transformation of the form $|E_N\rangle \mapsto |E'_N\rangle |\phi\rangle$, for some shared entangled state $|\phi\rangle$ of their choice, where $\{|E_N\rangle\}$ is a special family of states defined so that it is possible to perform such a transformation in which $|E_N\rangle \approx |E'_N\rangle$ for large N . Thus, they “embezzle” $|\phi\rangle$ from $|E_N\rangle$, leaving little trace of their crime. The process for doing this described by van Dam and Hayden is coherent and requires no communication, and can therefore be done twice (once in reverse) to achieve coherent state exchange. It relies, however, on a representation of two-party pure quantum states that no longer exists for m -party states when $m \geq 3$.

Here, we show that coherent state exchange for any number of parties is always possible, with near-perfect coherence. To simplify the description of the procedure, we will assume that $|\phi\rangle$ and $|\psi\rangle$ are orthogonal. (The more general case where $|\phi\rangle$ and $|\psi\rangle$ are not necessarily orthogonal is easily handled, and is discussed in the appendix.)

Let N be a positive integer, which will determine the accuracy of the procedure. We assume that each player P_i holds $N + 2$ identical registers labelled $X_{0,i}^1, \dots, X_{N+1,i}^1$, where each register has an associated Hilbert space that is isomorphic to \mathcal{X}^i . We take the initial state of the registers $(X_{1,1}^1, \dots, X_{1,1}^m), \dots, (X_{N+1,1}^1, \dots, X_{N+1,1}^m)$ to be

$$|E_N\rangle = \frac{1}{\sqrt{N}} \sum_{k=1}^N |\phi\rangle^{\otimes k} |\psi\rangle^{\otimes (N-k+1)}, \quad (1)$$

and we consider the case where the initial state of the registers $(X_{0,i}^1, \dots, X_{0,i}^m)$ is the input state $|\phi\rangle$. Thus, the state (1) represents the entanglement initially shared by P_1, \dots, P_m . The procedure that transforms $|\phi\rangle$ into $|\psi\rangle$ is simple: each player P_i cyclically shifts the contents of the registers $X_{0,i}^1, \dots, X_{N+1,i}^1$ by applying a unitary operation defined by the action

$$|x_0\rangle |x_1\rangle \cdots |x_{N+1}\rangle \mapsto |x_{N+1}\rangle |x_0\rangle \cdots |x_N\rangle$$

on standard basis states.

Let us now consider the properties of the above procedure. It is clear that after the cyclic shift, the registers $(X_{0,i}^1, \dots, X_{0,i}^m)$ will contain a perfect copy of $|\psi\rangle$, and the remaining registers will contain the state

$$|E'_N\rangle = \frac{1}{\sqrt{N}} \sum_{k=1}^N |\phi\rangle^{\otimes (k+1)} |\psi\rangle^{\otimes (N-k)}. \quad (2)$$

Thus, the procedure transforms $|\phi\rangle |E_N\rangle$ into $|\psi\rangle |E'_N\rangle$. It is easily checked that $\langle E'_N | E_N \rangle = 1 - 1/N$, so for large N there is only a small disturbance to the shared entangled state $|E_N\rangle$. The procedure satisfies the coherence requirement for this reason.

In the case that the players wished instead to transform $|\psi\rangle$ to $|\phi\rangle$, so that the initial state of the registers $(X_{0,i}^1, \dots, X_{0,i}^m)$ is $|\psi\rangle$, the same state (1) may be used, but the registers are shifted in the opposite direction.

Further connections to embezzlement and other work

A notion related to coherent state exchange, known as *catalytic transformation* of pure states, was considered by Jonathan and Plenio [JP99]. In particular, they considered the situation in which two parties transform one pure state to another (by local operations and classical communication) using a catalyst—or a state that assists but is left unchanged by the process. Coherent state exchange (and embezzlement) do almost exactly this, and without the exchange of classical information, but in the approximate sense that the catalyst is permitted to change slightly.

As mentioned above, in the case $m = 2$ one may use quantum state embezzlement twice to implement coherent state exchange. The family of states $\{|E_N\rangle\}$ defined in [DH03] also has the added property of being *universal*, or independent of the state $|\phi\rangle$ to be embezzled. We note that it is possible to use our method to give universal embezzling families for all m . To define a universal embezzling family for any fixed m , we may consider an ϵ -net of states $\{|\psi\rangle\}$ in N^m dimensions (for $\epsilon = 1/N$, say), take $|\phi\rangle = |0^m\rangle$, and define the embezzling state for each N to be the tensor product of all the states $|E_N\rangle$ ranging over the ϵ -net. The embezzlement of a particular state is then performed in the most straightforward way. Unlike the families of van Dam and Hayden for the case $m = 2$, our method is highly inefficient, but nevertheless establishes that universal embezzling families exist for all m .

3 Finite entanglement is suboptimal

The purpose of this section is to prove the first main result of the paper, which is that there exist two-prover quantum interactive proof systems for which no finite amount of entanglement allows for an optimal strategy on any fixed input. It suffices to define a two-prover quantum interactive proof system having no dependence on the input x ; or, in simpler terms, to consider a cooperative game played by two players and moderated by a referee. This type of *cooperative quantum game* represents a generalization of the *non-local games* model of [CHTW04], where now the referee can send, receive, and process quantum information.

To be more precise, and to aid in the exposition that follows, we define two-player, one-round cooperative quantum games as follows:

1. The referee prepares three quantum registers (R, S, T) in some chosen state, and then sends S to Alice and T to Bob.
2. Alice and Bob transform the registers S and T sent to them however they choose, resulting in registers A and B that are sent back to the referee.
3. The referee performs a binary-valued measurement on the registers (R, A, B) . The outcome 1 means that Alice and Bob win, while the outcome 0 means that they lose.

The restrictions on Alice and Bob are the same as for provers in a quantum interactive proof system: they are not permitted to communicate once the game begins, but may agree on a strategy beforehand. Such a strategy may include the sharing of an entangled state of their own choosing, which they may use when transforming the registers sent to them. The complexity of the referee, which corresponds to the verifier in an interactive proof system, is ignored given that we no longer consider an input string.

Description of the game

Consider the two-player cooperative quantum game that is determined by the following specification of the referee:

1. Let R be a qubit register and let S and T be qutrit registers. The referee initializes the registers (R, S, T) to the state

$$\frac{1}{\sqrt{2}} |0\rangle |00\rangle + \frac{1}{\sqrt{2}} |1\rangle |\phi\rangle$$

where

$$|\phi\rangle = \frac{1}{\sqrt{2}} |11\rangle + \frac{1}{\sqrt{2}} |22\rangle.$$

The registers S and T are sent to Alice and Bob, respectively.

2. The referee receives A from Alice and B from Bob, where A and B are both single-qubit registers. The triple (R, A, B) is measured with respect to the projective measurement $\{\Pi_0, \Pi_1\}$, where $\Pi_0 = I - |\gamma\rangle\langle\gamma|$ and $\Pi_1 = |\gamma\rangle\langle\gamma|$, for $|\gamma\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$. In accordance with the conventions stated above, the outcome 1 means that Alice and Bob win while 0 means that they lose.

The intuition behind this game is as follows. Alice and Bob are presented with two possibilities, in superposition: they receive either the unentangled state $|00\rangle$ or the entangled state $|\phi\rangle$. Their goal is essentially to do nothing to $|00\rangle$ and to convert $|\phi\rangle$ to $|11\rangle$, for they want the referee to hold the state $|\gamma\rangle$ when the final measurement is made. These transformations must be done coherently, without measurements or residual evidence of which of the two transformations $|00\rangle \mapsto |00\rangle$ or $|\phi\rangle \mapsto |11\rangle$ was performed, for otherwise the final state of the referee will not have a large overlap with $|\gamma\rangle$.

The required transformation will be possible using coherent state exchange, with a winning probability approaching 1. It will be shown, however, that it is never possible for Alice and Bob to win with certainty, provided they initially share a finite entangled state.

Strategies that win with probability approaching 1

We now present a family of strategies for Alice and Bob that win with probability approaching 1. In the above game, Alice receives S from the referee and returns A ; and likewise for Bob with registers T and B . Alice will begin with the qubit A initialized to $|0\rangle$, and Bob begins with B initialized to $|0\rangle$ as well. Let U be a unitary operation, acting on a pair consisting of a qutrit and a qubit, with the following behavior:

$$U : |0\rangle |0\rangle \mapsto |0\rangle |0\rangle, \quad U : |1\rangle |0\rangle \mapsto |1\rangle |1\rangle, \quad \text{and} \quad U : |2\rangle |0\rangle \mapsto |2\rangle |1\rangle.$$

Upon receiving S , Alice applies U to (S, A) , and Bob does likewise to (T, B) after receiving T . This leaves the 5-tuple (R, A, B, S, T) in the state

$$\frac{1}{\sqrt{2}} |000\rangle |00\rangle + \frac{1}{\sqrt{2}} |111\rangle |\phi\rangle.$$

Alice and Bob have not yet sent A and B to the referee. Before sending these registers, they use them as control qubits to transform registers S and T in superposition: if A and B are set to 0 then

nothing happens, while if A and B are 1 they perform coherent state exchange, transforming $|\phi\rangle$ to $|00\rangle$. Assuming that Alice and Bob initially share the entangled state

$$|E_N\rangle = \frac{1}{\sqrt{N}} \sum_{k=1}^N |\phi\rangle^{\otimes k} |00\rangle^{\otimes (N-k+1)},$$

the resulting state is

$$\frac{1}{\sqrt{2}} |000\rangle |00\rangle |E_N\rangle + \frac{1}{\sqrt{2}} |111\rangle |00\rangle |E'_N\rangle$$

for

$$|E'_N\rangle = \frac{1}{\sqrt{N}} \sum_{k=1}^N |\phi\rangle^{\otimes (k+1)} |00\rangle^{\otimes (N-k)}.$$

The registers A and B are now sent to the referee, whose measurement results in outcome 1 with probability

$$\left\| \frac{1}{2} |E_N\rangle + \frac{1}{2} |E'_N\rangle \right\|^2 = 1 - \frac{1}{2N}.$$

Impossibility to win with certainty

Now we will prove that Alice and Bob cannot win with certainty regardless of the strategy they employ. Without loss of generality, it may be assumed that Alice and Bob initially share a pure entangled state $|\psi\rangle \in \mathcal{X}_A \otimes \mathcal{X}_B$, where the spaces \mathcal{X}_A and \mathcal{X}_B have the same dimension d . When Alice and Bob receive S and T from the referee, the state of the entire system is given by

$$\frac{1}{\sqrt{2}} |0\rangle |00\rangle |\psi\rangle + \frac{1}{\sqrt{2}} |1\rangle |\phi\rangle |\psi\rangle.$$

General quantum operations performed by Alice and Bob can be described by linear isometries: A for Alice and B for Bob. These isometries take the form $A : \mathcal{S} \otimes \mathcal{X}_A \rightarrow \mathcal{A} \otimes \mathcal{Y}_A$ and $B : \mathcal{T} \otimes \mathcal{X}_B \rightarrow \mathcal{B} \otimes \mathcal{Y}_B$, where $\mathcal{S}, \mathcal{T}, \mathcal{A}, \mathcal{B}$ are the spaces associated with the registers S, T, A, and B, and the spaces \mathcal{Y}_A and \mathcal{Y}_B are arbitrary. The state of the system immediately before the referee measures is therefore

$$\frac{1}{\sqrt{2}} |0\rangle (A \otimes B) |00\rangle |\psi\rangle + \frac{1}{\sqrt{2}} |1\rangle (A \otimes B) |\phi\rangle |\psi\rangle.$$

By defining operators $A_0, A_1 \in \mathcal{L}(\mathcal{S} \otimes \mathcal{X}_A, \mathcal{Y}_A)$ and $B_0, B_1 \in \mathcal{L}(\mathcal{T} \otimes \mathcal{X}_B, \mathcal{Y}_B)$ as

$$A_0 = (\langle 0| \otimes I) A, \quad A_1 = (\langle 1| \otimes I) A, \quad B_0 = (\langle 0| \otimes I) B, \quad B_1 = (\langle 1| \otimes I) B,$$

we may express the probability that Alice and Bob win as

$$\frac{1}{4} \|(A_0 \otimes B_0) |00\rangle |\psi\rangle + (A_1 \otimes B_1) |\phi\rangle |\psi\rangle\|^2 \leq \frac{1}{2} + \frac{1}{2} |\langle \phi | \langle \psi | (A_1^* A_0 \otimes B_1^* B_0) |00\rangle |\psi\rangle|.$$

We have that $\|A_1^* A_0\| \leq 1$ and $\|B_1^* B_0\| \leq 1$, and therefore it is possible to express both $A_1^* A_0$ and $B_1^* B_0$ as convex combinations of unitary operators. By convexity, the winning probability is therefore bounded above by

$$\frac{1}{2} + \frac{1}{2} |\langle \phi | \langle \psi | (U_A \otimes U_B) |00\rangle |\psi\rangle|$$

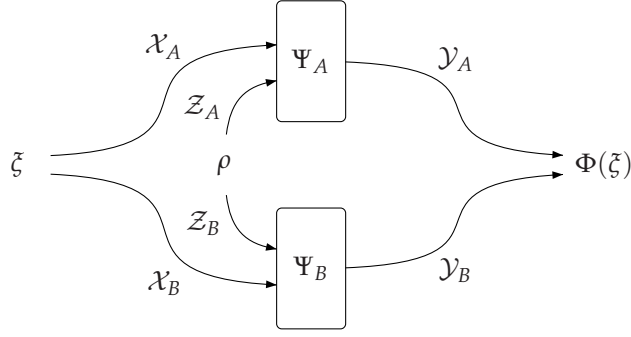


Figure 1: An entanglement-assisted local quantum operation Φ . An input state $\xi \in \mathcal{D}(\mathcal{X}_A \otimes \mathcal{X}_B)$ is transformed into the output state $\Phi(\xi)$ by means of local quantum operations Ψ_A and Ψ_B , along with a shared entangled state $\rho \in \mathcal{D}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$.

for some choice of unitary operators U_A and U_B . Notice that $(U_A \otimes U_B) |00\rangle |\psi\rangle$ must have 1 e-bit of entanglement less than $|\phi\rangle |\psi\rangle$, and so the states cannot be equal—and therefore the success probability cannot be 1.

A quantitative bound may be proved as follows. Using one of the Fuchs–van de Graaf inequalities [FvdG99] and the monotonicity of the fidelity under partial tracing, it holds that

$$|\langle \phi, \psi | U_A \otimes U_B | 00, \psi \rangle| \leq F(\rho, \xi) \leq \sqrt{1 - \frac{1}{4} \|\rho - \xi\|_1^2}$$

for

$$\begin{aligned} \rho &= \text{Tr}_{\mathcal{B} \otimes \mathcal{X}_B} (|\phi\rangle \langle \phi| \otimes |\psi\rangle \langle \psi|), \\ \xi &= \text{Tr}_{\mathcal{B} \otimes \mathcal{X}_B} U_A (|00\rangle \langle 00| \otimes |\psi\rangle \langle \psi|) U_A^*. \end{aligned}$$

At this point we may follow precisely the analysis of van Dam and Hayden [DH03] for the near-optimality of their universal embezzling families: we have that $S(\rho) - S(\xi) = 1$, from which it follows that $\|\rho - \xi\|_1 \geq 1/(2 \log(3d))$ by Fannes’ inequality [Fan73]. Consequently, the winning probability is bounded above by $1 - 1/(32 \log^2(3d))$. The error probability therefore decreases at most quadratically in the number of qubits that Alice and Bob initially share.

Consequences for entanglement assisted local quantum operations

For fixed spaces $\mathcal{X}_A, \mathcal{X}_B, \mathcal{Y}_A$, and \mathcal{Y}_B , a quantum operation $\Phi : \mathcal{L}(\mathcal{X}_A \otimes \mathcal{X}_B) \rightarrow \mathcal{L}(\mathcal{Y}_A \otimes \mathcal{Y}_B)$ is an *entanglement assisted local quantum operation* if it can be realized as illustrated in Figure 1; or more precisely, if there exists some choice of spaces \mathcal{Z}_A and \mathcal{Z}_B , a density operator $\rho \in \mathcal{D}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$, and admissible super-operators $\Psi_A : \mathcal{L}(\mathcal{X}_A \otimes \mathcal{Z}_A) \rightarrow \mathcal{L}(\mathcal{Y}_A)$ and $\Psi_B : \mathcal{L}(\mathcal{X}_B \otimes \mathcal{Z}_B) \rightarrow \mathcal{L}(\mathcal{Y}_B)$ such that $\Phi(\xi) = (\Psi_A \otimes \Psi_B)(\rho \otimes \xi)$ for all $\xi \in \mathcal{L}(\mathcal{X}_A \otimes \mathcal{X}_B)$. Operations of this type are also known as *localizable* operations [BGNP01]. In addition to having an obvious relevance to two-prover quantum interactive proof systems, this is an interesting and fundamental class of quantum operations in its own right.

An unfortunate fact that follows from the analysis of the game presented above is the following. When \mathcal{X}_A and \mathcal{X}_B have dimension at least 3 and \mathcal{Y}_A and \mathcal{Y}_B have dimension at least 2, the set of entanglement-assisted local quantum operations $\Phi : \mathcal{L}(\mathcal{X}_A \otimes \mathcal{X}_B) \rightarrow \mathcal{L}(\mathcal{Y}_A \otimes \mathcal{Y}_B)$ is not a

closed set: the sequence of entanglement-assisted local quantum operations induced by the strategies described above converges to a valid quantum operation that is not an entanglement-assisted local quantum operation.

Another connection with prior work

We wish to point out one further connection between the above result and some existing work. In the exact catalytic transformation setting of Jonathan and Plenio [JP99], Daftuar and Klimesh [DK01] proved the following fact: the dimension of the catalyst required to transform one state to another, when this is possible, cannot be bounded by any function of the dimension of those states. Although this fact does not have a direct implication to the cooperative quantum games model, and is incomparable to our result as far as we can see, there is a similarity in spirit between the results that is worthy of note.

4 Near-perfect completeness

Kempe, Kobayashi, Matsumoto, and Vidick [KKMV08] proved that multi-prover quantum interactive proof systems can be efficiently transformed to have *perfect completeness*, while retaining small soundness error. An analogous fact was previously shown to hold for single-prover quantum interactive proof systems [KW00], but the two proofs are quite different. The proof in [KW00] for the single-prover case is very simple while the proof in [KKMV08] for the multi-prover case is rather complicated. In this section we show that the use of coherent state exchange allows the simple proof for the single-prover setting to be applied in the multi-prover setting.

There is, however, one small caveat: whereas Kempe, Kobayashi, Matsumoto, and Vidick achieve truly perfect completeness (in as far as quantum operations can ever be implemented perfectly), we must settle for *near-perfect* completeness: similar to the game from the previous section, honest provers will be able to convince the verifier to accept yes-inputs with any probability smaller than 1 that they desire, but the probability may not in actuality be 1. For most intents and purposes, though, we believe that this behavior can reasonably be viewed as representing perfect completeness.

Suppose that a verifier V interacts with m provers P_1, \dots, P_m for r rounds, and suppose the completeness and soundness probabilities for this verifier are given by c and s , respectively (which may be functions of the input length). Specifically, for the promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ of interest, the following conditions hold:

1. **Completeness.** The verifier is convinced to accept every yes-input $x \in A_{\text{yes}}$ with probability at least $c(|x|)$ by the provers' strategy.
2. **Soundness.** The verifier cannot be convinced to accept any no-input $x \in A_{\text{no}}$ with probability exceeding $s(|x|)$, regardless of the provers' strategy.

As usual and without loss of generality, we may “purify” a given proof system so that the verifier V and provers P_1, \dots, P_m are described by unitary operations and the provers' initial shared entanglement is pure. We also make two simple assumptions on the proof system and the completeness probability $c(|x|)$. First, we assume that it is possible for the provers to convince the verifier to accept every string $x \in A_{\text{yes}}$ with probability exactly $c(|x|)$. This can be achieved, for example, by appending an extra bit to the last message of the first prover and having the verifier reject

when this bit is 1. Second, we assume that the value $c(|x|)$ is such that the verifier can efficiently implement the rotation

$$|0\rangle \mapsto \sqrt{1 - c(|x|)} |0\rangle - \sqrt{c(|x|)} |1\rangle, \quad |1\rangle \mapsto \sqrt{c(|x|)} |0\rangle + \sqrt{1 - c(|x|)} |1\rangle$$

without error. (We also assume reversible computations incur no error.)

Now, assume that an input string $x \in A_{\text{yes}} \cup A_{\text{no}}$ has been fixed. (As x is now fixed, we will not explicitly refer to x or $|x|$ when discussing quantities depending on x .) Let p denote the probability that the verifier accepts. Given the purity assumption of the proof system, this means that the final state of the entire system at the end of the interaction may be expressed as

$$\sqrt{1 - p} |0\rangle |\phi_0\rangle + \sqrt{p} |1\rangle |\phi_1\rangle,$$

where the first qubit in this expression represents the verifier's output qubit. The remaining part of the state, represented by $|\phi_0\rangle$ and $|\phi_1\rangle$, corresponds to the state of every other register in the proof system, shared in some arbitrary way among the verifier and provers. For simplicity we will assume that $|\phi_0\rangle$ and $|\phi_1\rangle$ are orthogonal, which at most requires that the verifier makes a pseudo-copy of the output qubit as its last action.

To transform the proof system to one with near-perfect completeness, one additional round of communication is added to the end of the protocol. To describe what happens in this additional round of communication, let us write A to denote the verifier's output qubit, V to denote the register comprising all of the verifier's memory aside from the output qubit, and P_1, \dots, P_m to denote registers representing the provers' memories, all corresponding to the final state of the original protocol.

To start the additional round of communication, the verifier prepares m additional single-qubit registers A_1, \dots, A_m as pseudo-copies of A , so that the state of the system becomes

$$\sqrt{1 - p} |0\rangle |0^m\rangle |\phi_0\rangle + \sqrt{p} |1\rangle |1^m\rangle |\phi_1\rangle.$$

The verifier then sends V to the first prover P_1 (which is an arbitrary choice, but one that all provers are aware of), and sends each register A_i to prover P_i .

Upon receiving these registers from the verifier, the provers perform the following actions. First, using the registers (A_1, \dots, A_m) as control qubits, the provers perform coherent state exchange: when each register A_i contains 0, nothing happens; and when each register A_i contains 1, the state $|\phi_1\rangle$ is exchanged for $|\phi_0\rangle$. The resulting state of the entire system is

$$\sqrt{1 - p} |0\rangle |0^m\rangle |\phi_0\rangle |E_N\rangle + \sqrt{p} |1\rangle |1^m\rangle |\phi_0\rangle |E'_N\rangle,$$

where

$$|E_N\rangle = \frac{1}{\sqrt{N}} \sum_{k=1}^N |\phi_0\rangle^{\otimes k} |\phi_1\rangle^{\otimes (N-k+1)}$$

is an additional shared entangled state the provers use for this purpose, and $|E'_N\rangle$ is defined in the same way as in Section 2. (This expression of $|E_N\rangle$ makes use of the assumption that $|\phi_0\rangle$ and $|\phi_1\rangle$ are orthogonal. One may instead consult the discussion in the appendix, which does not require this assumption.) The number N is the provers' choice for an accuracy parameter, which we assume to be as large as they wish. Once this is done, the provers return the registers A_1, \dots, A_m to the verifier.

The final step is that the verifier measures the registers (A, A_1, \dots, A_m) with respect to a basis containing the state $\sqrt{1 - c} |0\rangle |0^m\rangle + \sqrt{c} |1\rangle |1^m\rangle$, accepting if the output matches this state. (This

is possible given our assumptions on c .) In the case that $x \in A_{\text{yes}}$ the provers may take $p = c$, and so the acceptance probability is

$$\|(1 - c)|E_N\rangle + c|E'_N\rangle\|^2 \geq 1 - \frac{1}{2N}.$$

This is arbitrarily close to 1, given that the provers may take any value for N . In the case that $x \in A_{\text{no}}$ we have $p \leq s$, from which it is routine to show that the acceptance probability is at most

$$\left(\sqrt{s}\sqrt{c} + \sqrt{1-s}\sqrt{1-c}\right)^2 \leq 1 - (c - s)^2.$$

5 Conclusion

We have discussed two applications of coherent state exchange to the study of multi-prover quantum interactive proof systems.

The first application demonstrates that provers in a multi-prover quantum interactive proof system may not always have an optimal strategy when limited to finite entanglement. We view that the primary importance of this fact is that it will serve to better focus efforts on proving bounds on the amount of entanglement needed for *close-to-optimal* provers in multi-prover quantum interactive proofs—for such bounds can only exist in general for close-to-optimal and not optimal success probability.

The second application is a simple proof that multi-prover quantum interactive proof systems can be efficiently transformed to have near-perfect completeness by adding one round of communication. There is a trade-off between this proof and the proof of Kempe, Kobayashi, Matsumoto, and Vidick [KKMV08], which is that it is considerably simpler but cannot be said to achieve absolutely perfect completeness.

A few other applications of coherent state exchange have also been mentioned. In particular, we have proved that the collection of entanglement-assisted local quantum operations on systems of dimension 3 and higher is not a closed set, and we have proved that (highly inefficient) universal embezzling families exist for any number of parties. It remains to be seen to what extent such families can be made more efficient.

References

- [AB06] S. Arora and B. Barak. *Complexity Theory: A Modern Approach (Preliminary web draft)*, 2006.
- [ALM⁺98] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, 1998.
- [AS98] S. Arora and S. Safra. Probabilistic checking of proofs: a new characterization of NP. *Journal of the ACM*, 45(1):70–122, 1998.
- [BB84] C. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.
- [BBC⁺93] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and EPR channels. *Physical Review Letters*, 70(12):1895–1899, 1993.

- [BDSW96] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters. Mixed state entanglement and quantum error correction. *Physical Review A*, 54:3824–3851, 1996.
- [Bel64] J. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964.
- [BFL91] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.
- [BGNP01] D. Beckman, D. Gottesman, M. Nielsen, and J. Preskill. Causal and localizable quantum operations. *Physical Review A*, 64(5):52309, 2001.
- [BOGKW88] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: how to remove intractability assumptions. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 113–131, 1988.
- [Bra03] G. Brassard. Quantum communication complexity. *Foundations of Physics*, 33(11):1593–1616, 2003.
- [BSST02] C. Bennett, P. Shor, J. Smolin, and A. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. *IEEE Transactions on Information Theory*, 48(10):2637–2655, 2002.
- [BW92] C. Bennett and S. Wiesner. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992.
- [CGJ07] R. Cleve, D. Gavinsky, and R. Jain. Entanglement-resistant two-prover interactive proof systems and non-adaptive private information retrieval systems. Available as arXiv.org e-Print 0707.1729, 2007.
- [CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.
- [CHTW04] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th Annual IEEE Conference on Computational Complexity*, pages 236–249, 2004.
- [CSUU07] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay. Perfect parallel repetition theorem for quantum XOR proof systems. In *Proceedings of the 22nd Annual IEEE Conference on Computational Complexity*, pages 109–114, 2007.
- [DH03] W. van Dam and P. Hayden. Universal entanglement transformations without communication. *Physical Review A*, 67(6):060302, 2003.
- [DHW04] I. Devetak, A. Harrow, and A. Winter. A family of quantum protocols. *Physical Review Letters*, 93(23):230505, 2004.
- [Din07] I. Dinur. The PCP theorem by gap amplification. *Journal of the ACM*, 54(3), 2007.
- [DK01] S. Daftuar and M. Klimesh. Mathematical structure of entanglement catalysis. *Physical Review A*, 64(4):042314, 2001.
- [Eke91] A. Ekert. Quantum cryptography based on Bell’s theorem. *Physical Review Letters*, 67(6):661–663, 1991.

- [Fan73] M. Fannes. A continuity property of the entropy density for spin lattice systems. *Communications in Mathematical Physics*, 31(4):291–294, 1973.
- [FvdG99] C. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.
- [Gis07] N. Gisin. Bell inequalities: many questions, a few answers. Available as arXiv.org e-Print quant-ph/0702021, 2007.
- [Gol01] O. Goldreich. *Foundations of Cryptography: Volume 1 – Basic Tools*. Cambridge University Press, 2001.
- [HHL04] A. Harrow, P. Hayden, and D. Leung. Superdense coding of quantum states. *Physical Review Letters*, 92(18):187901, 2004.
- [JP99] D. Jonathan and M. Plenio. Entanglement-assisted local manipulation of pure quantum states. *Physical Review Letters*, 83(17):3566–3569, 1999.
- [KKM⁺07] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. Entangled games are hard to approximate. Available as arXiv.org e-Print 0704.2903, 2007.
- [KKMV08] J. Kempe, H. Kobayashi, K. Matsumoto, and T. Vidick. Using entanglement in quantum multi-prover interactive proofs. In *Proceedings of the 23rd Annual Conference on Computational Complexity*, 2008. To appear.
- [KM03] H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66(3), 2003.
- [KRT07] J. Kempe, O. Regev, and B. Toner. The unique games conjecture with entangled provers is false. Available as arXiv.org e-Print 0710.0655, 2007.
- [KW00] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof system. In *Proceedings of the 32nd ACM Symposium on Theory of Computing*, pages 608–617, 2000.
- [LC99] H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050–2056, 1999.
- [SP00] P. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, 2000.
- [Weh06] S. Wehner. Entanglement in interactive proof systems with binary answers. In *Proceedings of the 23rd Annual Symposium on Theoretical Aspects of Computer Science*, volume 3884 of *Lecture Notes in Computer Science*, pages 162–171. Springer, 2006.
- [Wol02] R. de Wolf. Quantum communication and complexity. *Theoretical Computer Science*, 287(1):337–353, 2002.

A Coherent exchange of non-orthogonal states

Here we briefly discuss coherent state exchange for non-orthogonal states $|\phi\rangle$ and $|\psi\rangle$. The simplest method that we have considered requires that

$$\dim(\mathcal{X}^1 \otimes \cdots \otimes \mathcal{X}^m) \geq 3,$$

which is immediate provided that $m \geq 2$ and that each \mathcal{X}^i is non-trivial. One may then choose any state $|\eta\rangle \in \mathcal{X}^1 \otimes \cdots \otimes \mathcal{X}^m$ that is orthogonal to both $|\phi\rangle$ and $|\psi\rangle$, and perform two state exchanges: first from $|\phi\rangle$ and $|\eta\rangle$ and then from $|\eta\rangle$ to $|\psi\rangle$. The auxiliary state naturally takes the form $|E_N\rangle |F_N\rangle$, where $|E_N\rangle$ is used to transform $|\phi\rangle$ to $|\eta\rangle$ and $|F_N\rangle$ is used to transform $|\eta\rangle$ to $|\psi\rangle$. Aside from this change, no new analysis is required.

Another method is as follows. Suppose $\langle\phi|\psi\rangle = ae^{i\theta}$ for $a > 0$, and define $|\tilde{\psi}\rangle = e^{-i\theta} |\psi\rangle$. It is easy to coherently exchange $|\tilde{\psi}\rangle$ for $|\psi\rangle$ by letting one player induce a global phase (which translates into a phase shift on a control qubit if the process is performed in superposition). Thus, it remains to exchange $|\phi\rangle$ for $|\tilde{\psi}\rangle$. If $a = 1$ there is nothing to do, while if $a < 1$ this may be done in a similar way to the orthogonal case, through the use of the state

$$|E_N\rangle = \frac{1}{\sqrt{N_1}} \sum_{k=1}^N |\phi\rangle^{\otimes k} |\tilde{\psi}\rangle^{\otimes (N-k+1)}.$$

The only difference between this state and the one in (1) is the normalization—it is obvious that $N \leq N_1 \leq N^2$, and more explicitly we have

$$N_1 = \frac{1+a}{1-a} N - 2a \frac{1-a^N}{(1-a)^2}.$$

For

$$|E'_N\rangle = \frac{1}{\sqrt{N_1}} \sum_{k=1}^N |\phi\rangle^{\otimes k+1} |\tilde{\psi}\rangle^{\otimes (N-k)}$$

we have

$$\langle E'_N | E_N \rangle = 1 - \frac{1-a^N}{N_1} \leq 1 - \frac{1}{N}.$$

As is not surprising, the efficiency is no worse than in the orthogonal case.